

# ENCIPHERING METHOD, APPARATUS AND PROGRAM

**Publication number:** JP2007150780 (A)

**Publication date:** 2007-06-14

**Inventor(s):** KIKUCHI HIROSHI; TAKAHASHI TATSUAKI; KIKUCHI TORU +

**Applicant(s):** CB KK +

**Classification:**

- international: **H04L9/08; H04L9/08**

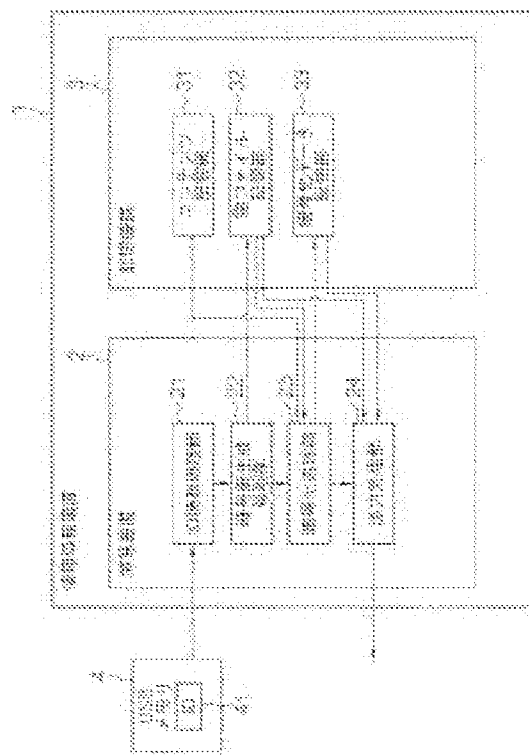
- European:

**Application number:** JP20050343174 20051129

**Priority number(s):** JP20050343174 20051129

## Abstract of **JP 2007150780 (A)**

**PROBLEM TO BE SOLVED:** To improve the reliability of the enciphering of electronic data with a simple method. ; **SOLUTION:** The method for enciphering the electronic data in a computer comprises: an equipment information read step of having the computer read identification information intrinsic to prescribed equipment equipped in the computer stored beforehand in the equipment; a cipher key information generation step of having the computer generate cipher key information on the basis of the read identification information; and an enciphering step of having the computer generate enciphered data by enciphering the electronic data by using the cipher key information. ; **COPYRIGHT:** (C)2007,JPO&INPIT



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-150780

(P2007-150780A)

(43) 公開日 平成19年6月14日(2007.6.14)

(51) Int.Cl.

H04L 9/08 (2006.01)

F1

H04L 9/00 G01A

テーマコード(参考)

5J104

審査請求 未請求 請求項の数 10 O L (全 13 頁)

(21) 出願番号

特願2005-343174 (P2005-343174)

(22) 出願日

平成17年11月29日(2005.11.29)

(71) 出願人

505263579

株式会社シービー

東京都港区芝4-5-15クレール芝302号

(74) 代理人

100124811

弁理士 馬場 資博

(72) 発明者

菊地 宏

東京都港区芝4-5-15 クレール芝302 株式会社シービー内

(72) 発明者

高橋 達昭

東京都港区芝4-5-15 クレール芝302 株式会社シービー内

(72) 発明者

菊地 亨

東京都港区芝4-5-15 クレール芝302 株式会社シービー内

最終頁に続く

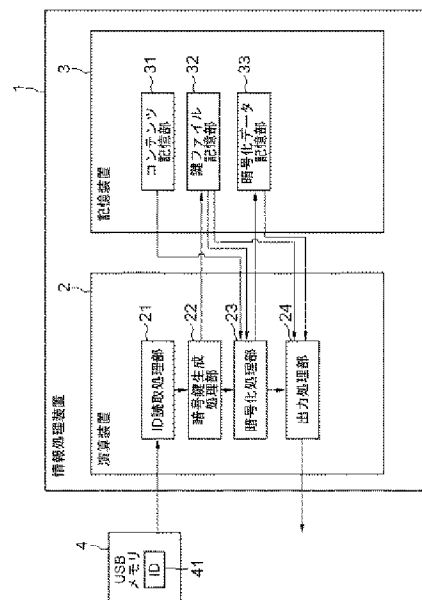
(54) 【発明の名称】 暗号化方法及び装置並びにプログラム

(57) 【要約】

【課題】簡易な方法にて電子データの暗号化の信頼性の向上を図ること。

【解決手段】コンピュータにて電子データの暗号化を行う方法であって、コンピュータが、当該コンピュータに装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取工程と、コンピュータが、読み取った識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成工程と、コンピュータが、暗号鍵情報を用いて電子データを暗号化して暗号化データを生成する暗号化工程と、を有する。

【選択図】図1



**【特許請求の範囲】****【請求項1】**

コンピュータにて電子データの暗号化を行う方法であって、  
前記コンピュータが、当該コンピュータに装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取工程と、  
前記コンピュータが、読み取った前記識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成工程と、  
前記コンピュータが、前記暗号鍵情報を用いて前記電子データを暗号化して暗号化データを生成する暗号化工程と、  
を有することを特徴とする暗号化方法。

**【請求項2】**

前記暗号化工程は、前記暗号鍵情報を用いて復号可能なよう前記電子データを暗号化する、ことを特徴とする請求項1記載の暗号化方法。

**【請求項3】**

前記暗号化工程の前に、前記コンピュータが、他のコンピュータに装備された所定の機器に固有の識別情報に基づいて当該他のコンピュータにて生成された第2暗号鍵情報を当該他のコンピュータから取得する第2暗号鍵情報取得工程を有し、  
前記暗号化工程は、暗号鍵情報生成工程にて生成された前記暗号鍵情報と前記第2暗号鍵情報取得工程にて取得された前記第2暗号鍵情報とに基づいて、前記電子データを暗号化して暗号化データを生成する、  
ことを特徴とする請求項1記載の暗号化方法。

**【請求項4】**

前記暗号化工程は、前記暗号鍵情報と前記第2暗号鍵情報とを用いて復号可能なよう前記電子データを暗号化する、ことを特徴とする請求項3記載の暗号化方法。

**【請求項5】**

電子データの暗号化を行う暗号化装置であって、  
暗号化装置に装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取手段と、  
読み取った前記識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成手段と、  
前記暗号鍵情報を用いて前記電子データを暗号化して暗号化データを生成する暗号化手段と、  
を備えたことを特徴とする暗号化装置。

**【請求項6】**

他の装置に装備された所定の機器に固有の識別情報に基づいて当該他の装置にて生成された第2暗号鍵情報を当該他の装置から取得する第2暗号鍵情報取得手段を備え、  
前記暗号化手段は、前記暗号鍵情報生成手段にて生成された前記暗号鍵情報と前記第2暗号鍵情報取得手段にて取得された前記第2暗号鍵情報とに基づいて、前記電子データを暗号化する、  
ことを特徴とする請求項5記載の暗号化装置。

**【請求項7】**

電子データの暗号化を行う暗号化用コンピュータに、  
暗号化用コンピュータに装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取手段と、  
読み取った前記識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成手段と、  
前記暗号鍵情報を用いて前記電子データを暗号化して暗号化データを生成する暗号化手段と、  
を実現するためのプログラム。

**【請求項8】**

前記暗号化用コンピュータに、

他の装置に装備された所定の機器に固有の識別情報に基づいて当該他の装置にて生成された第2暗号鍵情報を当該他の装置から取得する第2暗号鍵情報取得手段と、

前記暗号鍵情報生成手段にて生成された前記暗号鍵情報と前記第2暗号鍵情報取得手段にて取得された前記第2暗号鍵情報とに基づいて、前記電子データを暗号化する前記暗号化手段と、

を実現するための請求項7記載のプログラム。

【請求項9】

コンピュータにて電子データの暗号化を行う方法であって、

前記コンピュータが、当該コンピュータに接続されたバイオメトリクス情報取得手段に入力された操作者固有の身体的特徴情報を読み取るバイオメトリクス情報読取工程と、

前記コンピュータが、読み取った前記身体的特徴情報に基づいて暗号鍵情報を生成する暗号鍵情報生成工程と、

前記コンピュータが、前記暗号鍵情報を用いて前記電子データを暗号化して暗号化データを生成する暗号化工程と、

を有することを特徴とする暗号化方法。

【請求項10】

前記暗号化工程の前に、前記コンピュータが、他の操作者固有の身体的特徴情報に基づいて生成された第2暗号鍵情報を取得する第2暗号鍵情報取得工程を有し、

前記暗号化工程は、前記暗号鍵情報生成工程にて生成された前記暗号鍵情報と前記第2暗号鍵情報取得工程にて取得された前記第2暗号鍵情報とに基づいて、前記電子データを暗号化する、

ことを特徴とする請求項9記載の暗号化方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、暗号化方法にかかり、特に、暗号鍵を用いて暗号化する暗号化方法に関する。また、暗号化装置及びプログラムに関する。

【背景技術】

【0002】

コンピュータの普及により、種々の情報を電子データにて扱うことが増えている。そして、個人的な情報や機密情報などの重要な情報は、不特定多数の者に利用されては困るため、特定の者にのみ電子データの利用（閲覧など）が可能なよう、暗号化されることが行われている。

【0003】

暗号化方法としては、例えば、以下の方法がある。まず、ユーザはコンピュータなどにパスワード（例えば「abc123」）を入力すると、コンピュータはそのパスワードを基に暗号鍵を生成する。そして、コンピュータでは、暗号鍵を用いて所定の暗号化アルゴリズムにて、暗号する対象の電子データを暗号化（エンコード）する。その後は、暗号化された電子データが配布されるが、配布先のコンピュータでは、上記暗号鍵を用いて、あるいは、上記暗号鍵に対応した復号鍵を用いて、復号（デコード）を行う。このとき、上記パスワードの入力を受けて、暗号鍵あるいは復号鍵が正しいかどうかを認証してもよい。

【0004】

また、上述した暗号化時におけるパスワードの入力を省略し、暗号化操作を容易にしつつ、セキュリティを確保した暗号化方法が下記の特許文献1に開示されている。この特許文献1に開示の技術では、上記パスワードに相当する顧客を識別する顧客識別データを予めUSBメモリなどに格納しておき、暗号鍵生成時にUSBメモリから顧客識別データを読み出して暗号化を行う、という技術である。

【0005】

【特許文献1】特開2005-275112号公報

【発明の開示】

**【発明が解決しようとする課題】****【0006】**

しかしながら、上記従来例に開示された暗号化方法では、いずれもユーザが任意に設定するパスワードから暗号化鍵を生成しているため、かかるパスワードの漏洩や盗聴などされたり、上記パスワードが解析されてしまうことも生じうる。すると、意図しない他人に暗号化された電子データを復号されてしまうおそれがあり、セキュリティが低下する、という問題が生じる。

**【0007】**

このため、本発明では、上記従来例の有する不都合を改善し、特に、簡易な方法にて電子データの暗号化の信頼性の向上を図ることができる暗号化方法を提供する、ことをその目的とする。

**【課題を解決するための手段】****【0008】**

そこで、本発明の一形態である暗号化方法は、  
コンピュータにて電子データの暗号化を行う方法であって、  
コンピュータが、当該コンピュータに装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取工程と、

コンピュータが、読み取った識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成工程と、

コンピュータが、暗号鍵情報を用いて電子データを暗号化して暗号化データを生成する暗号化工程と、  
を有することを特徴としている。

**【0009】**

そして、上記暗号化工程は、暗号鍵情報を用いて復号可能なよう電子データを暗号化する、ことを特徴としている。

**【0010】**

上記発明によると、まず、コンピュータは、当該コンピュータに内蔵されたハードディスクや、当該コンピュータに接続されたUSBメモリなどのハードウェア（機器）から、当該ハードウェアに記憶されているシリアルナンバーなどの固有の識別情報を読み取る。続いて、コンピュータは、読み取った識別情報に基づいて予め設定された処理にて暗号鍵を生成し、暗号鍵ファイルとして記憶しておく。続いて、暗号化を行う電子データをハードディスクなどから読み出し、この電子データを上記暗号鍵ファイルを用いて暗号化して暗号化データを生成する。このとき、暗号化処理に用いる暗号化アルゴリズムは任意である。その後、暗号化データが特定の相手に配布されると共に、暗号鍵ファイルも配布され、この暗号鍵ファイルを用いることで、暗号化データを復号することができる。

**【0011】**

これにより、他人は暗号化データを入手したとしても、これを復号することは困難である。つまり、暗号鍵をユーザ端末に装備されたハードウェアに固有の識別情報を利用して生成したため、数学的に暗号鍵の解読が困難となり、また、パスワードを用いていないことから、その漏洩や盗聴の心配もなくなる。その結果、ユーザは特別な操作を行うことなく、簡易な操作にて暗号化の信頼性の向上を図ることができる。

**【0012】**

さらに、暗号鍵には、暗号化するコンピュータに装備されたハードウェアに固有の識別情報が記憶されているため、暗号化したコンピュータ端末を特定することができる。

**【0013】**

また、暗号化工程の前に、コンピュータが、他のコンピュータに装備された所定の機器に固有の識別情報に基づいて当該他のコンピュータにて生成された第2暗号鍵情報を当該他のコンピュータから取得する第2暗号鍵情報取得工程を有し、

暗号化工程は、暗号鍵情報生成工程にて生成された暗号鍵情報と第2暗号鍵情報取得工程にて取得された第2暗号鍵情報とに基づいて、電子データを暗号化して暗号化データを

生成する、  
ことを特徴としている。

【0014】

さらに、暗号化工程は、暗号鍵情報と第2暗号鍵情報とを用いて復号可能なよう電子データを暗号化する、ことを特徴としている。

【0015】

上記発明によると、暗号化を行うコンピュータは、他のコンピュータにて上述同様にハードウェア（機器）固有の識別情報を用いて生成された第2暗号鍵情報を取得し、記憶する。その後、暗号化を行うコンピュータにて生成された暗号鍵情報と、上記取得した第2の暗号鍵情報と、を用いて電子データを暗号化し、暗号化データを生成する。その後、暗号化データが例えば他のコンピュータに配布されると共に、暗号化を行ったコンピュータにて生成された暗号鍵ファイルも送られる。すると、他のコンピュータでは、受け取った暗号鍵ファイルと、既に生成して記憶している第2暗号鍵ファイルと、を用いて暗号化データを復号することができる。

【0016】

これにより、上述したように、ハードウェアに固有の識別情報を利用して生成した暗号鍵を2つ保持していないと復号できないため、さらなるセキュリティの強化を図ることができる。また、復号時には、他のコンピュータにて生成された第2暗号鍵を保有している必要があるため、復号可能な端末を特定することも可能となる。

【0017】

また、本発明の他の形態である暗号化装置は、電子データの暗号化を行う暗号化装置であって、暗号化装置に装備された所定の機器に予め記憶された当該機器に固有の識別情報を読み取る機器情報読取手段と、読み取った識別情報に基づいて暗号鍵情報を生成する暗号鍵情報生成手段と、暗号鍵情報を用いて電子データを暗号化して暗号化データを生成する暗号化手段と、を備えたことを特徴としている。

【0018】

そして、上記暗号化装置は、さらに、他の装置に装備された所定の機器に固有の識別情報に基づいて当該他の装置にて生成された第2暗号鍵情報を当該他の装置から取得する第2暗号鍵情報取得手段を備え、暗号化手段は、暗号鍵情報生成手段にて生成された暗号鍵情報と第2暗号鍵情報取得手段にて取得された第2暗号鍵情報とに基づいて、電子データを暗号化する、ことを特徴としている。

【0019】

さらに、本発明では、電子データの暗号化を行う暗号化用コンピュータに、上述した暗号化装置が備える各手段を実現するためのプログラムをも提供している。このように、上記構成の暗号化装置、プログラムであっても、上述した暗号化方法と同様の作用を有するため、上記本発明の目的を達成することができる。

【0020】

また、本発明の他の形態である暗号化方法は、  
コンピュータにて電子データの暗号化を行う方法であって、  
コンピュータが、当該コンピュータに接続されたバイオメトリクス情報取得手段に入力された操作者固有の身体的特徴情報を読み取るバイオメトリクス情報読取工程と、  
コンピュータが、読み取った身体的特徴情報に基づいて暗号鍵情報を生成する暗号鍵情報生成工程と、  
コンピュータが、暗号鍵情報を用いて電子データを暗号化して暗号化データを生成する暗号化工程と、  
を有することを特徴としている。

【0021】

そして、暗号化工程の前に、コンピュータが、他の操作者固有の身体的特徴情報に基づいて生成された第2暗号鍵情報を取得する第2暗号鍵情報取得工程を有し、

暗号化工程は、暗号鍵情報生成工程にて生成された暗号鍵情報と第2暗号鍵情報取得工

程にて取得された第2暗号鍵情報とに基づいて、電子データを暗号化する、ことを特徴としている。

【0022】

上記発明によると、まず、コンピュータは、バイオメトリクス情報取得手段に入力されたコンピュータの操作者の指紋・手形・網膜・虹彩・声紋・顔・署名・手の甲の静脈パターンなどの身体的特徴情報を読み取り、この身体的特徴情報に基づいて予め設定された処理にて暗号鍵を生成し、暗号鍵ファイルとして記憶しておく。続いて、暗号化を行う電子データをハードディスクなどから読み出し、この電子データを上記暗号鍵ファイルを用いて暗号化して暗号化データを生成する。その後、暗号化データが特定の相手に配布されると共に、暗号鍵ファイルも配布され、この暗号鍵ファイルを用いることで、暗号化データを復号することができる。また、他の操作者の身体的特徴情報に基づいて生成された第2暗号鍵ファイルを取得して、上述同様に、2つの暗号鍵ファイルを用いて暗号化することも可能である。

【0023】

これにより、暗号鍵を操作者固有の身体的特徴情報を用いて生成したため、数学的に暗号鍵の解読が困難となり、また、パスワードを用いていないことから、その漏洩や盗聴の心配もなくなり、他人は暗号化ファイルを入手したとしても、これを復号することは困難となる。その結果、ユーザは特別な操作を行うことなく、簡易な操作にて電子データの暗号化の信頼性の向上を図ることができる。また、暗号化した操作者を特定したり、復号可能な人を特定することも可能である。

【発明の効果】

【0024】

本発明は、以上のように構成され機能するので、これによると、暗号鍵をユーザ端末に装備されたハードウェアに固有の識別情報や、操作者固有の身体的特徴情報を利用して生成したため、数学的に暗号鍵の解読が困難となり、また、パスワードを用いていないことから、その漏洩や盗聴の心配もなくなる。このため、他人は暗号化データを入手したとしても、これを復号することは困難となり、その結果、ユーザは特別な操作を行うことなく、簡易な操作にて暗号化の信頼性の向上を図ることができる、という従来にない優れた効果を有する。

【発明を実施するための最良の形態】

【0025】

本発明は、暗号化する際に用いる暗号鍵を、ユーザ端末に装備されたハードウェアに固有の識別情報や、操作者固有の身体的特徴情報を利用して生成し、これを用いて暗号化することに特徴を有する。以下、実施例1、2では、ハードウェア固有の識別情報を用いて暗号鍵を生成する場合を説明し、実施例3では、操作者固有の身体的特徴情報を利用して暗号鍵を生成する場合を説明する。なお、いずれの実施例においても、入力される識別情報が異なるだけであって、その他の構成や動作は共通する。

【実施例】

【0026】

本発明の第1の実施例を、図1乃至図2を参照して説明する。図1は、暗号化処理を行う情報処理装置の構成を示す機能ブロック図であり、図2は、その動作を示すフローチャートである。

【0027】

〔構成〕

実施例1における暗号化処理を行う情報処理装置は、図1に示すように、CPUなどの演算装置2と、ハードディスクなどの記憶装置3と、を備えた一般的なコンピュータである。そして、この情報処理装置1に、所定の記憶媒体に格納された暗号化用プログラムが提供され、組み込まれることで、演算装置2には、ID読取処理部21、暗号鍵生成処理部22、暗号化処理部23、出力処理部24、が構築される。また、記憶装置3には、コンテンツ記憶部31、鍵ファイル記憶部32、暗号化データ記憶部33が形成されている。

。以下、各処理部21～24、各記憶部31～33について詳述する。

【0028】

ID読取処理部21（機器情報読取手段）は、情報処理装置1に装備された機器に予め記憶された当該機器に固有の識別情報を読み取る。例えば、図1に示すように、情報処理装置1のUSB接続端子に接続されたUSBメモリ4から、このハードウェア固有のシリアルナンバーなどのID41を読み取る。なお、情報処理装置1に内蔵されたCPUやハードディスク、あるいは、外付けされたプリンタなど、いかなるハードウェアから固有のIDを読み取ってもよい。

【0029】

暗号鍵生成処理部22（暗号鍵情報生成手段）は、上記USBメモリ4から読み取ったID41を用いて、予め設定された演算式にて暗号鍵を生成する。そして、生成した暗号鍵（バイナリデータ）をファイル形式で、暗号鍵ファイルとして鍵ファイル記憶部32に記憶する。

【0030】

暗号化処理部23（暗号化手段）は、まず、文書ファイルなどの電子データを記憶したコンテンツ記憶部31から、暗号化の対象となる電子データを読み出す。そして、上記鍵ファイル記憶部32から暗号鍵ファイルを読み出して、この暗号鍵ファイルを用いて電子データを予め設定された暗号化アルゴリズムにて暗号化し、暗号化データを生成する。なお、このとき、暗号化処理時に使用した暗号鍵ファイルを用いることで復号が可能なよう暗号化処理する。そして、生成した暗号化データを暗号化データ記憶部33に記憶しておく。

【0031】

出力処理部24は、暗号化データ記憶部33に格納されている暗号化データを、特定のユーザに対して配布するよう出力する。例えば、配布可能な記憶媒体に出力したり、ネットワークを介して相手先の情報処理端末に送信する。さらに、この出力処理部24は、鍵ファイル記憶部32に記憶されている暗号鍵ファイルを、上述した暗号化データを配布するユーザに対して配布するよう出力する。例えば、暗号化データを予め特定のユーザに対して配布しておき、その後、配布したい電子データが生じたときには、この電子データを既に配布した暗号鍵ファイルを用いて暗号化し、その暗号化データを同じ特定のユーザに対して配布する。

【0032】

〔動作〕

次に、上記構成の情報処理装置1の動作を、図2を参照して説明する。まず、情報処理装置1は、接続されたUSBメモリ4に予め設定されているID41を読み取る（ステップS1、機器情報読取工程）。続いて、情報処理装置1は、読み取ったID41に基づいて暗号鍵を生成し、暗号鍵ファイルとして記憶しておく（ステップS2、暗号鍵情報生成工程）。続いて、暗号化を行う電子データを読み出し（ステップS3）、この電子データを暗号鍵ファイルを用いて暗号化して暗号化データを生成し、記憶する（ステップS4、S5、暗号化工程）。

【0033】

その後、暗号化データが特定の相手に配布されると共に（ステップS6）、暗号鍵ファイルも配布される（ステップS7）。なお、暗号鍵ファイルは、事前に配布されていてもよい。すると、配布先の情報処理端末では、配布を受けた暗号化データの復号を、同様に配布された暗号鍵ファイルを用いて行うことができる。つまり、暗号化した情報処理装置1で生成され、暗号化処理に用いられた暗号鍵ファイルを渡した相手だけが復号可能になる。従って、暗号鍵ファイルを渡す相手を管理制限することで、1対n（nは任意の整数）での暗号化データの受け渡しや、特定のグループ内や階層別グループでの暗号化データの受け渡しが可能となる。

【0034】

以上より、本発明によると、仮に他人が暗号化データを不正に入手したとしても、暗号

鍵を所定のハードウェアに固有のパラメータを利用して生成したため、数学的に暗号鍵の解読が困難となる。また、パスワードを用いていないことから、その漏洩や盗聴の心配もなくなり、ユーザは特別な操作を行うことなく、簡易な操作にて信頼性の高い暗号化を行うことができる。

【0035】

さらに、暗号鍵には、暗号化する情報処理装置1に装備されたハードウェアに固有の識別情報が記憶されているため、暗号化した情報処理装置1を特定することができる。すると、配布された暗号化データや暗号鍵ファイルが信頼できるユーザから配布されたデータであるかどうかの確認も行うことができる。

【実施例】

【0036】

次に、本発明の第2の実施例を、図3乃至図4を参照して説明する。図3は、暗号化処理を行う情報処理装置の構成を示す機能ブロック図であり、図4は、その動作を示すフローチャートである。

【0037】

〔構成〕

実施例2における暗号化処理を行う情報処理装置5（自端末）は、上述した実施例1における情報処理装置1とほぼ同様の構成を備えている。つまり、情報処理装置5に、所定の記憶媒体に格納された暗号化用プログラムが提供され組み込まれることで、演算装置6には、ID読取処理部61、暗号鍵生成処理部62、暗号化処理部63、出力処理部64、が構築され、さらに、暗号鍵取得処理部65が構築される。また、記憶装置7には、コンテンツ記憶部71、鍵ファイル記憶部72、暗号化データ記憶部75が形成されている。以下、各処理部61～65、各記憶部71～75について詳述する。

【0038】

ID読取処理部61、暗号鍵生成処理部62は、実施例1の場合とほぼ同様に作動し、情報処理装置5に接続されたUSBメモリ8から読み取ったID81を用いて、暗号鍵ファイルを生成する。このとき、生成した暗号鍵（バイナリデータ）をファイル形式で、第1鍵73（第1の暗号鍵ファイル）として鍵ファイル記憶部72に記憶する。

【0039】

また、暗号鍵取得処理部65（第2暗号鍵情報取得手段）は、他の情報処理装置9（他端末）にて生成された暗号鍵ファイル、つまり、第2鍵91（第2暗号鍵情報）を、ネットワークNを介して取得し、鍵ファイル記憶部72に第2鍵74として記憶する。このとき、第2鍵91は、他の情報処理装置9に装備されたハードウェアに固有の識別情報（ID）に基づいて、当該他の情報処理装置9にて生成されたものである。すなわち、他の情報処理装置9には、上述したID読取処理部及び暗号鍵生成処理部と同様の機能が備わっている。なお、暗号鍵取得処理部65は、必ずしもネットワークNを介して第2鍵を取得することに限定されず、所定の記憶媒体に格納された状態で提供された第2鍵を読み取るにより取得してもよい。

【0040】

暗号化処理部63は、まず、文書ファイルなどの電子データを記憶したコンテンツ記憶部71から、暗号化の対象となる電子データを読み出す。そして、鍵ファイル記憶部72から、自端末5にて生成した第1鍵73（暗号鍵ファイル）と、他端末9にて生成され取得した第2鍵74（第2の暗号鍵ファイル）と、を読み出して、2つの暗号鍵ファイルを用いて電子データを暗号化し、暗号化データを生成する。なお、このとき、暗号化処理時に使用した2つの暗号鍵ファイルを用いることで復号が可能なよう暗号化処理する。そして、生成した暗号化データを暗号化データ記憶部75に記憶しておく。

【0041】

出力処理部64は、暗号化データ記憶部75に格納されている暗号化データを、特定のユーザ、例えば、ネットワークNを介して他の情報処理端末9に対して配布するよう出力する。さらに、この出力処理部64は、鍵ファイル記憶部72に記憶されている第1鍵7

3 (暗号鍵ファイル) を、他の情報処理端末9に対しても配布する。これにより、他の情報処理端末9には、取得した第1鍵73と、事前に生成して記憶している第2鍵91と、が保持され、復号時に用いられる。なお、暗号化データをさらに他の情報処理端末に配布する場合には、第1鍵73及び第2鍵74も配布する必要がある。

【0042】

〔動作〕

次に、上記構成の各情報処理装置5、9の動作を、図4を参照して説明する。まず、暗号化処理を行う自端末側Aでは、情報処理装置5が接続されたUSBメモリ8からID81を読み取る(ステップS11、S12、機器情報読取工程)。そして、読み取ったID81に基づいて暗号鍵を生成し、暗号鍵ファイル(第1鍵73)として記憶しておく(ステップS13、暗号鍵情報生成工程)。

【0043】

同様に、任意の時期に、他の情報処理端末9(他端末側B)は、当該他の情報処理装置9に内蔵されたハードディスク10(他のハードウェアでもよい)からIDを読み取り(ステップS21、S22)、読み取ったIDに基づいて暗号鍵を生成し、暗号鍵ファイル(第2鍵91)として記憶しておく(ステップS23)。

【0044】

その後、自端末側Aの情報処理装置5は、他の情報処理装置9に対して暗号鍵ファイルを要求し(ステップS31)、これに応じて他の情報処理装置9はステップS23で生成した第2鍵91を、自端末側Aの情報処理装置5に送信する(ステップS32)。そして、自端末側Aの情報処理装置5は、取得した第2鍵を記憶保持する(ステップS33、第2暗号鍵情報取得工程)。これにより、自端末側Aの情報処理装置5には、第1鍵73と第2鍵74が保持された状態になる。

【0045】

続いて、自端末側Aの情報処理装置5が暗号化を行う際には、暗号化を行う電子データを読み出すと共に、第1鍵73、第2鍵74を読み出し、電子データを2つの暗号鍵ファイルを用いて暗号化して暗号化データを生成し、記憶する(ステップS34、暗号化工程)。

【0046】

その後、暗号化データが他の情報処理装置9に配布されると共に(ステップS35)、第1鍵73である暗号鍵ファイルも配布される(ステップS36)。なお、暗号鍵ファイルは、事前に配布されていてもよい。すると、配布先となる他の情報処理装置9では、配布を受けた暗号化データの復号を、同様に配布された第1鍵と、予め保持している第2鍵と、を用いて行うことができる。つまり、暗号化した情報処理装置5で生成され、暗号化処理に用いられた第1鍵を渡した相手であり、かつ、自身で生成した第2鍵を有する他の情報処理装置9のみが、暗号化データを復号することができる。従って、強固な1対1の暗号化を行うことができ、より確実に復号可能な端末を特定することができる。

【実施例】

【0047】

次に、本発明の第3の実施例を、図5を参照して説明する。図5は、暗号化処理を行う情報処理装置の構成を示す機能ブロック図である。

【0048】

本実施例における暗号化処理を行う情報処理装置100には、当該情報処理装置100の操作者140から、指紋・手形・網膜・虹彩・声紋・顔・署名・手の甲の静脈パターンなどの身体的特徴情報(バイオメトリクス情報)を読み取るセンサ部131を備えた読取装置130(バイオメトリクス情報取得手段)が接続されている。

【0049】

また、情報処理装置100は、上述した実施例1における情報処理装置1とほぼ同様の構成を備えている。つまり、情報処理装置100に、所定の記憶媒体に格納された暗号化用プログラムが提供され組み込まれることで、演算装置110には、バイオメトリクス情

報読取処理部111、暗号鍵生成処理部112、暗号化処理部113、出力処理部114、が構築されている。そして、記憶装置120には、コンテンツ記憶部121、鍵ファイル記憶部122、暗号化データ記憶部123が形成されている。

【0050】

上記バイオメトリクス情報取得処理部111は、読取装置130に入力された操作者140固有のバイオメトリクス情報を取得し、暗号化鍵生成処理部112に渡す。そして、暗号化鍵生成処理部112は、このバイオメトリクス情報を用いて、暗号鍵ファイルを作成する。このとき、生成した暗号鍵（バイナリデータ）をファイル形式で暗号鍵ファイルとして鍵ファイル記憶部122に記憶する。なお、その他の処理部113、114の構成は、上記実施例と同様である。

【0051】

これにより、まず、情報処理装置100は、操作者140固有のバイオメトリクス情報を読み取り（バイオメトリクス情報読取工程）、この固有の情報に基づいて暗号鍵ファイルを作成する（暗号鍵情報生成工程）。その後、上述同様に、この暗号鍵ファイルを用いて、当該暗号鍵ファイルにて復号可能なよう、所定の電子データを暗号化して暗号化データを生成する（暗号化工程）。つまり、実施例1におけるハードウェア固有の識別情報に換えて、操作者固有のバイオメトリクス情報を用いた場合でも、上述同様に、簡易な操作、つまり、バイオメトリクス情報を読み取らせるという操作にて、信頼性の高い暗号化データを生成することができる。

【0052】

なお、上述した実施例2の場合にも、ハードウェア固有の識別情報に換えて、各情報処理装置5、9の各操作者固有のバイオメトリクス情報を用いてもよい。つまり、まず、暗号化を行う情報処理装置5では、第1の操作者から入力されたバイオメトリクス情報を用いて第1鍵を生成し、他の情報処理装置9では、第2の操作者から入力された各バイオメトリクス情報を用いて第2鍵を生成する。そして、上述したように、暗号化を行う情報処理装置5が他の情報処理装置9から第2鍵を取得して、2つの暗号鍵を用いて暗号化を行う。その他の動作は、実施例2の場合と同様である。

【産業上の利用可能性】

【0053】

本発明は、情報処理装置に組み込んで電子データを暗号化して暗号化データを生成することに利用することができ、産業上の利用可能性を有する。

【図面の簡単な説明】

【0054】

【図1】実施例1における情報処理装置の構成を示す機能ブロック図である。

【図2】実施例1における暗号化時の動作を示すフローチャートである。

【図3】実施例2における情報処理装置の構成を示す機能ブロック図である。

【図4】実施例2における暗号化時の動作を示すシーケンス図である。

【図5】実施例3における情報処理装置の構成を示す機能ブロック図である。

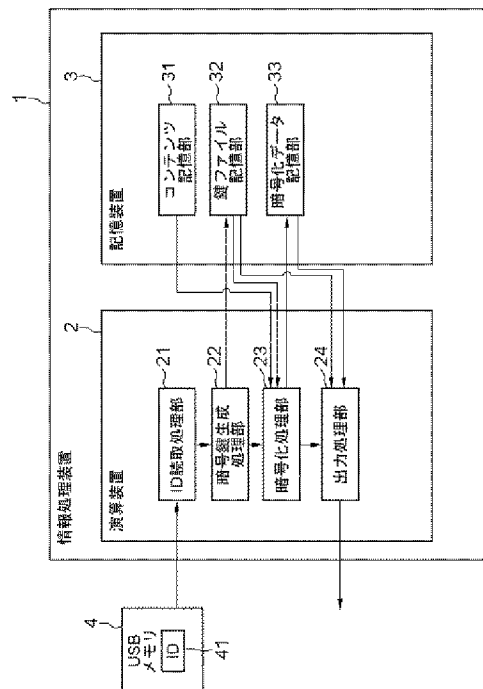
【符号の説明】

【0055】

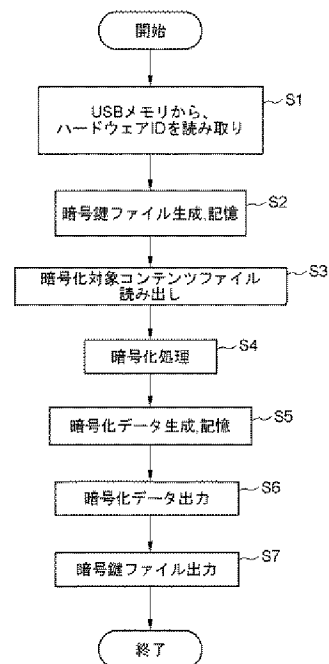
- 1, 5, 100 情報処理装置（暗号化装置）
- 4 USBメモリ（機器）
- 9 他端末
- 21, 61 ID読取処理部（機器情報読取手段）
- 22, 62, 112 暗号鍵生成処理部（暗号鍵情報生成手段）
- 23, 63, 113 暗号化処理部（暗号化手段）
- 24, 64, 114 出力処理部
- 31, 71, 121 コンテンツ記憶部
- 32, 72, 122 鍵ファイル記憶部
- 33, 75, 123 暗号化データ記憶部

- 41, 81 ID (識別情報)  
 65 暗号鍵取得処理部 (第2暗号鍵情報取得手段)  
 73 第1鍵  
 74, 91 第2鍵  
 130 読取装置 (バイオメトリクス情報取得手段)  
 140 操作者

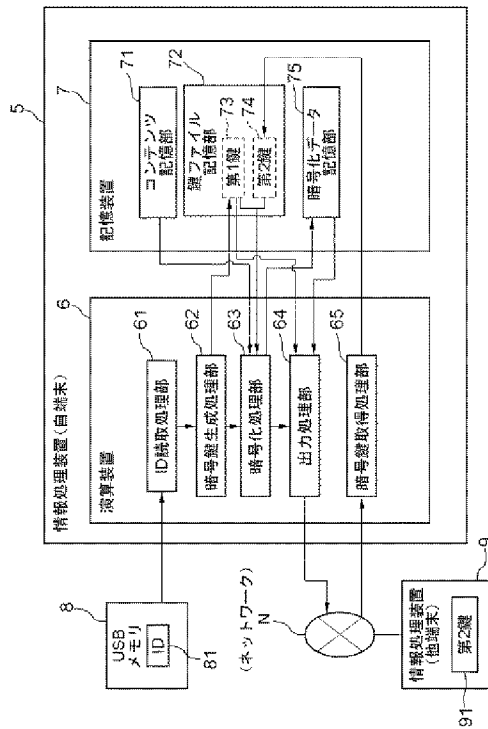
【図1】



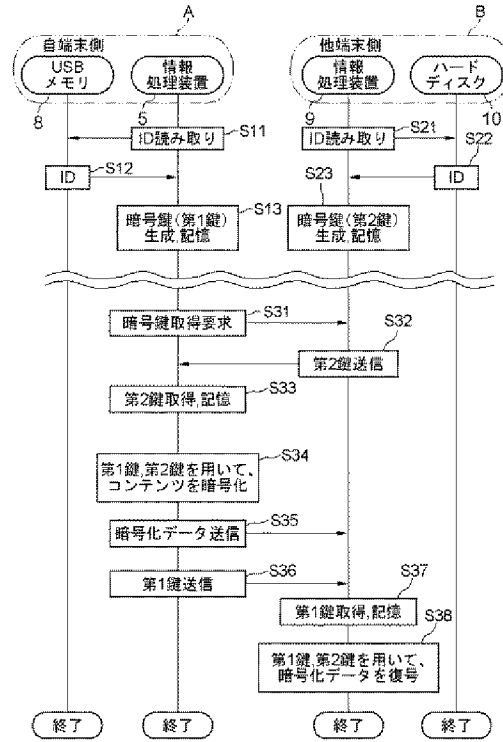
【図2】



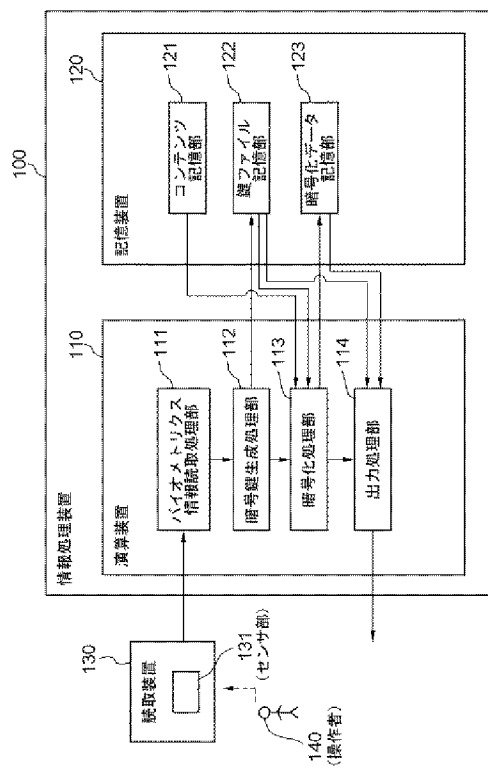
【図3】



【図4】



【図5】



Fターム(参考) 5J104 AA16 AA32 EA04 EA15 EA16 JA03 NA02 NA27 NA37 PA14